EXHIBIT B

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NORTH CAROLINA

DENNIS HANSCOM,

On Behalf of Himself and All Others Similarly Situated,

Plaintiff,

v.

NORDSEC LTD., NORDSEC B.V., NORDVPN S.A., NORD SECURITY INC., and TEFINCOM S.A. d/b/a NordVPN,

Defendants.

Case No. 3:24-CV-277-KDB-DCK

AMENDED CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Dennis Hanscom ("Plaintiff"), by his undersigned attorneys, Milberg Coleman Bryson Phillips Grossman, PLLC and Wittels McInturff Palikovic, brings this consumer protection action in his individual capacities and on behalf of a class of consumers defined below against Defendants NordSec Ltd., NordSec B.V., Nordvpn S.A., Nord Security Inc., and Tefincom S.A. d/b/a NordVPN (hereafter, "Defendants," "Nord Security," or the "Company") and hereby alleges the following with knowledge as to his own acts and upon information and belief as to all other acts:

INTRODUCTION

1. This is a proposed class action lawsuit challenging Nord Security's use of deceptive and illegal tactics to trick consumers into paying for unwanted, pricey subscriptions for internet security services. Nord Security intentionally misleads consumers into thinking they can easily "try" NordSec's virtual private network and other services "risk-free" before becoming full-fledged subscribers. The truth is, however, that Nord Security's "risk-free" trial is hard to cancel and is designed to ensnare customers and cause unintended purchases once the trial period ends.

2. Nord Security offers a suite of products and services to consumers that claim to provide internet users with privacy and protection from cybersecurity threats. Those offerings include a virtual private network ("VPN") service called "NordVPN," [1] a password manager called "NordPass," and an encrypted cloud storage service called "NordLocker."

3. Potential customers are directed to Nord Security's various sales websites through online searches, its sponsorship of influencers, or by advertising for the Company's VPN and/or

[1] A VPN service is one that purports to protect a user's internet connection and online privacy. These services typically route a user's internet traffic through an encrypted tunnel to a server in another location, masking the user's location and protecting the user's data from interception along the way. Uses for VPNs range from casual entertainment (i.e., using a VPN while abroad to watch a show that is only available in the U.S.) to the distribution of politically significant information (i.e., masking journalistic sources within a totalitarian regime).

other services. Nord Security advertises widely online and on dozens of podcasts. Nord Security's advertising touts the benefits that its services allegedly offer the prudent consumer; for example, the Company claims that its VPN service provides consumers "safe and private access to the internet" and that it is "trusted by tech experts and users."

4. While consumers are told they can "try" Nord Security's privacy and security products and services before becoming full-fledged customers, unbeknownst to these consumers, Nord Security is actually collecting consumers' payments and payment information via illegal and deceptive subscription practices designed to make the "risk-free" trial a trap for the unwary.

5. Nord Security's supposedly "risk-free" trials are offered with a "negative option" feature, which the Consumer Financial Protection Bureau ("CFPB") defines as "a term or condition under which a seller may interpret a consumer's silence, failure to take an affirmative action to reject a product or service, or failure to cancel an agreement as acceptance or continued acceptance of the offer."[2] As the CFPB notes, "[n]egative option programs can cause serious harm to consumers," which "is most likely to occur when sellers mislead consumers about terms and conditions, fail to obtain consumers' informed consent, or make it difficult for consumers to cancel."[3]

6. That is exactly what happened here. Due to Nord Security's deceptive and unlawful negative option practices, many consumers who sign up for a Nord Security service ultimately end up paying for subscriptions that they do not want.

THE UNIFORM WEB OF NORDSEC'S NEGATIVE OPTION SCHEME

7. Nord Security traps consumers into becoming full-fledged customers with a web of

[2] Consumer Financial Protection Circular 2023-01, Unlawful negative option marketing practices (Jan. 19, 2023), https://files.consumerfinance.gov/f/documents/cfpb_unlawful-negative-option-marketing-practices-circular_2023-01.pdf.

[3] *Id*. at 2.

deceptive online design features that exploit well-known shortcomings in consumer decision-making. The paragraphs below describe the various ways in which Nord Security employs deception in the structure of its supposedly "risk-free" trial offering. While Nord Security's deceptive web has several components that can independently trip up consumers and lead to inadvertent purchases, taken together these components make up a larger deceptive process that leads to a common and predictable outcome: saddling consumers with accidental subscriptions.

8. Nord Security does so in at least five ways.

9. First, Nord Security lures customers with deceptive promises that they can "try" its "cutting-edge technology" services "risk-free" and that if the consumer decides during the trial period that Nord Security is not the right fit, the consumer can simply "cancel anytime" during a 30-day window and "get your money back." The pitch is simple: Nord Security is so confident in its "trusted" security services that it is willing to let consumers "try" them with "no risk" by giving them refunds with "no hassle" if they cancel during that trial period.

10. Yet "cancelling" a Nord Security trial within the 30-day window does ***not*** result in a "no hassle" refund, a fact which is not made apparent to reasonable consumers. Instead of simply cancelling within the window, to get the promised refund a trial-period customer needs to both "cancel" within the 30-day trial program ***and also*** affirmatively request a refund within that same 30-day period—despite Nord Security's promise that the consumer can "cancel anytime before [the end of the 30-day trial period] and get your money back." By imposing an additional, unexpected step in its supposedly "risk-free" trial Nord Security deceptively withholds refunds from customers who cancel during the "risk-free" trial. To make matters worse, Nord Security saddles consumers with the cost of a full year (or more) of its services if they do not complete this second and unexpected refund request step.

11. Second, during the trial-period enrollment process, Nord Security fails to clearly and conspicuously disclose that the trial automatically renews into a full-fledged subscription (that itself also automatically renews). Specifically, Nord Security fails to clearly and conspicuously disclose the terms of the automatic renewal offer before consumers commit to the supposedly "risk-free" trial, including how to cancel. For example, instead of clearly explaining to the consumer what they are actually getting into, Nord Security requires customers to scroll to find the relevant (and inadequate) fine print on its payment page and buries the key provisions in confusing, inconsistent, and inaccurate terms scattered across multiple sections of at least two fine print documents.

12. Third, Nord Security's scheme continues post-sign up. The Company's acknowledgement emails sent to consumers after they sign up for the trail fail to inform consumers that they must take affirmative steps beyond cancellation during the trial period to obtain a refund or what those steps are, and fails to provide written notice that the customer's subscription will automatically renew at least 15 days, but no earlier than 45 days, before the subscription automatically renews, as required by North Carolina law.

13. Fourth, Nord Security makes canceling exceedingly difficult and requires customers to figure out—with no help from the Company—that to Defendants, cancelling means the entirely unorthodox process of navigating Nord Security's account settings to find a buried feature labelled "Auto-renewal" and turning it to "OFF" (rather than, for example, by clicking a button clearly and prominently labelled, "CANCEL SUBSCRIPTION"). And for those consumers who contact the Company directly prior to the end of their current trial or subscription period to cancel, Nord Security refuses to cancel any upcoming payments and instead only turns off autorenewal for later payments.

14. Fifth, Nord Security employs a highly unconventional charging practice. Rather than automatically renew consumers by charging their stored payment methods at the beginning of a new subscription period if they do not cancel before the prior subscription is over, Nord Security extracts its charges 14 days ***before the customer's current subscription period even ends***. By doing so, Nord Security locks consumers into another yearlong subscription well before any reasonable consumer would expect to be auto-renewed, allowing Nord Security to collect and keep payment from consumers who do not wish to remain Nord Security customers.

15. Again, while a given customer may not be ensnared by each and every aspect of Nord Security's deceptive subscription web, all Nord Security customers face the same traps and need only be tricked by one of them to end up paying a hefty subscription fee for a year (or more) of internet security and privacy services they do not want.

16. These outcomes are not only unsurprising, they are also the result of intentional and bad-faith design choices. Defendants are well aware that their scheme is tricking consumers, as complaints about Nord Security are legion, with hundreds of consumers complaining on sites like Trustpilot, SiteJabber, and Reddit or directly to Nord Security. Upon information and belief, Nord Security experiences a high rate of chargebacks when consumers, frustrated by Nord Security's subscription practices, initiate disputes through their credit card companies or other payment processors over unwanted Nord Security transactions. Upon information and belief, Nord Security has developed customer service protocols for dealing with customers complaining about unwanted subscription charges.

17. Nevertheless, despite the clear messages Defendants' customers are sending them, Nord Security continues to subject the consuming public to its unlawful subscription scheme and Defendants continue to reap significant monetary benefits from it.

18. Only through a class action can consumers remedy Defendants' unlawful practices. Because the monetary damages suffered by each customer are small compared to the much higher cost a single customer would incur in trying to challenge Nord Security's improper conduct, it makes no financial sense for an individual customer to bring his or her own lawsuit. Furthermore, many customers do not realize they are victims of Nord Security's unlawful acts and continue to be charged to this day. With this class action, Plaintiff and the Class seek to level the playing field, enjoin Nord Security's unlawful business practices, and recover the charges Nord Security has imposed on Plaintiff and the Class in violation of the law.

JURISDICTION AND VENUE

19. This Court has personal jurisdiction over Defendants because they conduct substantial business in North Carolina, have sufficient minimum contacts with this state, and otherwise purposely avail themselves of the privileges of conducting business in North Carolina by marketing and selling products and services in North Carolina. Further, the injuries to North Carolina consumers that Plaintiff seeks to prevent through public injunctive relief arise directly from Nord Security's continuing conduct in North Carolina, including, but not limited to, directing its subscription practices at North Carolina consumers.

20. This Court has jurisdiction over the claims asserted in this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because the aggregate claims of the Class exceed the sum or value of $5,000,000, the Class has more than 100 members, and diversity of citizenship exists between at least one member of the Class and Defendants.

21. This Court has original subject matter jurisdiction over all claims in this action pursuant to the Class Action Fairness Act. However, if the Court determines that it lacks original jurisdiction over any claim in this action, it may exercise supplemental jurisdiction over Plaintiff's

claims under 28 U.S.C. § 1367 because all of the claims arise from a common nucleus of operative facts and are such that Plaintiff ordinarily would expect to try them in one judicial proceeding.

22. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b). Substantial acts in furtherance of the alleged improper conduct occurred within this District, as Plaintiff resides in this District, and Defendants reside in this District for venue purposes. *Id.* at § 1391(c)(2).

PARTIES

23. Plaintiff Dennis Hanscom is a citizen of North Carolina and lives in Charlotte, North Carolina. He enrolled in a Nord Security subscription on August 2, 2023.

24. Plaintiff is a consumer who was victimized by Nord Security's unlawful autorenewal practices, suffered injury in fact, and lost money because of Nord Security's violations of North Carolina consumer protection statutes.

25. Upon information and belief, with respect to all actions and decisions relevant to this action, Defendants have operated as a single company called "Nord Security." Yet unbeknownst to the ordinary consumer, "Nord Security," is a brand and not a corporate entity.

26. Defendants hold themselves out to the public, including Plaintiff, as if a single fictitious entity called "Nord Security" sells the services consumers in North Carolina and the rest of the United States purchase. For example, when a consumer visits www.nordsecurity.com they see a typical company website that features "our products" (including the products purchased by Plaintiff), "our story," "our team" and "our values." Similarly, when top U.S. venture capital firm Warburg Pincus and others invested $100 million in Defendants, "Nord Security" issued a press release describing the funding as an investment in "Nord Security, a global leader in internet privacy and security solutions."[4] This same press release states that NordVPN is "the biggest and

[4] Nord Security raised another $100M investment round, NORD SECURITY, https://nordsecurity.com/blog/nord-security-raised-another-100m-investment-round.

most popular VPN service in the world" and that "Nord Security was founded in Lithuania in 2012 by co-founders and co-CEOs Tom Okman and Eimantas Sabaliauskas."[5] Likewise, the "Corporate responsibility" page for "Nord Security" shows pictures of the founders and explains "our mission," and contains links to Nord Security's "corporate responsibility reports" and Nord Security's "Code of Conduct,"[6] which discusses such topics as expectations for the "Nord Security brand products, including NordVPN, NordPass, NordLocker, and NordLayer."[7]

27. Defendant NordSec Ltd. is an internet privacy and security company headquartered in London, England.[8] NordSec Ltd. is a citizen of the United Kingdom.[9] Defendants claim that NordSec Ltd. "once owned the intellectual property of the Nord brand."[10] NordSec's corporate parents are Cyberswift B.V., Cyberspace B.V., and Stalwart Holding B.V.[11] NordSec Ltd. is also an owner of Defendant NordSec B.V., Defendant Nordvpn S.A., and Defendant Nord Security Inc. Public records indicate that NordSec Ltd. is a prior owner of the "NordVPN" trademark.

28. Defendant NordSec B.V. is an internet privacy and security company headquartered in Amsterdam, the Netherlands.[12] NordSec B.V. is a citizen of the Netherlands.[13] Defendants claim that NordSec B.V. "currently owns the intellectual property" of the Nord

---

[5] *Id.*

[6] Corporate Responsibility, NORD SECURITY, https://nordsecurity.com/corporate-responsibility

[7] Code of Conduct, NORD SECURITY, https://res.cloudinary.com/nordsec/image/upload/v1712078877/nord-security-web/corporate/code%20of%20conduct/Nord_Security_Code_of_Conduct.pdf.

[8] ECF No. 45-1, ¶ 3.

[9] ECF No. 39.

[10] ECF No. 45-1, ¶ 3.

[11] ECF No. 35.

[12] ECF No. 45-2, ¶ 3.

[13] ECF No. 41.

brand.[14] NordSec B.V.'s corporate parents are Defendant NordSec Ltd. and two of that Defendant's corporate parents, Cyberswift B.V. and Cyberspace B.V.[15] NordSec B.V. is also an owner of Defendant Nordvpn S.A. and Defendant Nord Security Inc. Defendants' website www.nordsecurity.com claims that "Nord Security trademarks, trade names, company names, logos," whether registered or not, "as well as other Nord Brand features (such as Nord Security websites, applications and creative works embodied therein), are the exclusive property of NordSec B.V. ('Nord Security')."[16] NordSec B.V.'s marks include the marks "Nord Security," "NordVPN," "Nord," "NordSec," NordLocker," and "NordPass." Upon information and belief, the website Plaintiff used to enroll with Nord Security was the website owned by Defendant NordSec B.V. and the Nord Security products he purchased bore the marks owned by Defendant NordSec B.V.

29. Defendant Nordvpn S.A. is a Panamanian corporation incorporated under the laws of Panama and its principal place of business is in Amsterdam, the Netherlands.[17] Nordvpn S.A. is a citizen of Panama and the Netherlands.[18] Nordvpn S.A. currently "offers" Defendants' products "NordVPN, NordLocker, and NordPass,"[19] which are the products Defendants marketed and sold to Plaintiff in North Carolina. Defendant Nordvpn S.A. also currently operates Defendants' website, www.nordvpn.com.[20] Nordvpn S.A.'s corporate parents are Defendant NordSec B.V., Defendant NordSec Ltd, and Cyberswift B.V., which is one of the corporate parents

[14] ECF No. 45, at 5.

[15] ECF No. 37.

[16] Nord Security Trademark and Brand Guidelines, NORD SECURITY, https://nordsecurity.com/trademark-policy.

[17] ECF No. 45-3, ¶ 3.

[18] ECF No. 40.

[19] ECF No. 45-3, ¶ 3.

[20] *Id.*

of Defendant NordSec Ltd.[21] Nordvpn S.A. shares an unnamed director with Defendant Tefincom S.A.[22]

30. Defendant Nord Security Inc. is a Delaware corporation.[23] Nord Security Inc.'s corporate parents are Defendant NordSec B.V., Defendant NordSec Ltd., and Cyberswift B.V., which is also a corporate parent of Defendants NordSec B.V. and NordSec Ltd.[24] Defendants claim that Nord Security Inc. is not the "Nord Security" that offers services to North Carolina consumers, instead claiming that Defendant Nord Security Inc. provides only business-to-business services.[25]

31. Defendant Tefincom S.A. is a Panamanian corporation incorporated under the laws of Panama.[26] Tefincom S.A.'s principal place of business is Panama City, Panama.[27] Defendant Tefincom S.A.'s corporate parent is Stitching Raveset.[28] Defendants admit that Defendant Tefincom S.A. was the contracting entity for North Carolina retail consumer VPN services purchased on or before November 15, 2020.[29] Defendant Tefincom S.A. was the original owner of the trademark for "NordVPN."

32. Upon information and belief, at all times pertinent to this action, the finances, policies, and business practices of Defendants are and were dominated and controlled by one

[21] ECF No. 36.

[22] ECF No. 45-3, ¶ 8.

[23] ECF No. 15.

[24] ECF No. 14.

[25] ECF No. 45, at 6.

[26] ECF No. 42.

[27] ECF No. 45-4, ¶ 3.

[28] ECF No. 38.

[29] ECF No. 45, at 6.

another in such a manner that each individual Defendant has no separate mind, will, identity, or existence of its own and instead operated as mere instrumentalities and alter egos of one another. For example, even though public records and fine print on the www.nordsecurity.com website indicate that Defendant NordSec B.V. owns the "NordVPN" trademark, one of Defendants' other websites states that "NordVPN is owned and operated by nordvpn S.A."[30] Similarly, that same website also states that "[b]ack in 2012, two best friends sought to create a tool for a safer and more accessible internet. Driven by the idea of internet freedom, Tom Okman and Eimantas Sabaliauskas created NordVPN."[31] Tom Okman and Eimantas Sabaliauskas are listed as directors of Defendant NordSec Ltd., but their respective LinkedIn pages claim they are co-founders of "Nord Security."[32]

33. Upon information and belief, Defendants are so closely related in ownership and management, and each works closely in concert with the other, such that each has become the alter ego of the other, in that, among others:

a. Defendants operate and hold themselves out to the public as a single, fictitious entity, Nord Security.

b. Defendants operate and hold themselves out to the public in such a way that members of the public would be unable to identify and distinguish between one entity and another. For example, a consumer searching the internet for "NordVPN" would find www.nordvpn.com, which is owned and operated by Defendant Nordvpn S.A. but which Defendants represent is owned by the non-existent entity "Nord Security." "Nord Security" is a trademark owned by Defendant NordSec B.V. The www.nordsecurity.com website, which Defendants also represent is owned by the brand "Nord Security" similarly lists the various "Nord Security" products, including NordVPN, NordLocker, and NordPass.

c. Defendants do not market themselves independently.

[30] The founders and owners of NordVPN, NORDVPN, https://support.nordvpn.com/hc/en-us/articles/20911146148113-The-founders-and-owners-of-NordVPN.

[31] *Id.*

[32] *See* https://www.linkedin.com/in/tokmanas/; *see also* https://www.linkedin.com/in/eimis/.

d. Olga Sinkeviciene, a director of NordSec Ltd., and Ruta Gorelcionkiene, a director of NordSec B.V., are both employees of CEOcorp, a company that "specializes in the incorporation of entities and implementation of corporate structures across diverse jurisdictions."[33]

e. Upon information and belief, Defendants share employees. For example, the LinkedIn pages of many of Defendants' employees state that these employees work at "Nord Security," even though no such entity exists. When a prospective employee visits Defendant Nordvpn S.A.'s website www.nordvpn.com they are redirected to the "careers" subpage of www.nordsecurity.com (https://nordsecurity.com/careers). That page contains various claims and a video about what it is like to work at "Nord Security." Job applicants can apply for "Nord Security" positions available in Lithuania, Germany, Poland, and remotely.

f. When Defendants issue press releases, they do so under the name "Nord Security" without identifying or distinguishing between corporate entities.

g. On information and belief, there is a unified executive team that controls all operational and financial aspects of Defendants.

34. All Defendants are represented by the same counsel in this case.

35. All Defendants do business in North Carolina under the name "Nord Security" and interacted with Plaintiff in North Carolina such that his claims described herein arise from Plaintiff's contacts with Defendants in North Carolina.

36. Any such conduct of one Defendant should be imputed to each other Defendant.

FACTUAL ALLEGATIONS

A. Background on the Subscription e-Commerce Industry

37. The e-commerce subscription model is a business model in which retailers provide ongoing goods or services "in exchange for regular payments from the customer."[34] Subscription e-commerce services target a wide range of customers and cater to a variety of specific interests. Given the prevalence of online and e-commerce retailers, subscription e-commerce has grown

[33] Services, CEOCORP, https://ceocorp.net/services/.

[34] *See* Sam Saltis, *How to Run an eCommerce Subscription Service: The Ultimate Guide*, CORE DNA, https://www.coredna.com/blogs/ecommerce-subscription-services.

rapidly in popularity in recent years. Indeed, the "subscription economy has grown more than 400% over the last 8.5 years as consumers have demonstrated a growing preference for access to subscription services[.]"[35] According to the Washington Post, analysts at UBS predict the subscription economy will expand into a $1.5 trillion market by 2025, up from $650 billion in 2020.[36]

38. The production, sale, and distribution of subscription-based products and services is a booming industry that has exploded in popularity over the past few years. "Over the past 11 years, subscription-based companies[] have grown 3.7x faster than the companies in the S&P 500."[37]

39. The expansion of the subscription e-commerce market shows no signs of slowing. According to The Washington Post, "[s]ubscriptions boomed during the coronavirus pandemic as Americans largely stuck in shutdown mode flocked to digital entertainment[.] . . . The subscription economy was on the rise before the pandemic, but its wider and deeper reach in nearly every industry is expected to last, even after the pandemic subsides in the United States."[38]

40. However, there are well-documented downsides associated with the subscription-based business model. While the subscription e-commerce market has low barriers and is thus easy to enter, it is considerably more difficult for retailers to dominate the market due to the "highly

[35] Mary Mesienzahl, *Taco Bell's taco subscription is rolling out nationwide — here's how to get it*, BUSINESS INSIDER (Jan. 6, 2022), https://www.businessinsider.com/taco-bell-subscription-launching-across-the-country-2022-1. (internal quotation marks omitted).

[36] Heather Long and Andrew Van Dam, *Everything's becoming a subscription, and the pandemic is partly to blame*, WASHINGTON POST (Jun. 1, 2021), https://www.washingtonpost.com/business/2021/06/01/subscription-boom-pandemic/.

[37] *The Subscription Economy Index*, ZUORA (Mar. 2023), https://www.zuora.com/wp-content/uploads/2023/03/Zuora_SEI_2023_Q2.pdf.

[38] Heather Long and Andrew Van Dam, *supra* note 35.

competitive prices and broad similarities among the leading players."[39] In particular, retailers struggle with the fact that "[c]hurn rates are high, [] and consumers quickly cancel services that don't deliver superior end-to-end experiences."[40] Yet, retailers have also recognized that, where the recurring nature of the service, billing practices, or cancellation process is unclear or complicated, "consumers may lose interest but be too harried to take the extra step of canceling their membership[s]."[41] As these companies have realized, "[t]he real money is in the inertia."[42] As a result, "[m]any e-commerce sites work with third-party vendors to implement more manipulative designs."[43] That is, to facilitate consumer inertia, some subscription e-commerce companies, including Defendants, "are now taking advantage of subscriptions in order to trick users into signing up for expensive and recurring plans. They do this by intentionally confusing users with their app's design and flow, … and other misleading tactics[,]" such as failure to fully disclose the terms of its automatic-renewal programs.[44]

41. To make matters worse, once enrolled in the subscription, "[o]ne of the biggest complaints consumers have about brand/retailers is that it's often difficult to discontinue a

---

[39] *Thinking inside the subscription box: New research on e-commerce consumers*, MCKINSEY & COMPANY (Feb. 2018), https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/thinking-inside-the-subscription-box-new-research-on-ecommerce-consumers#0.

[40] *Id.*

[41] Amrita Jayakumar, *Little-box retailing: Subscription services offer new possibilities to consumers, major outlets*, WASHINGTON POST (Apr. 7, 2014), https://www.washingtonpost.com/business/economy/tktktktk/2014/04/07/f68135b6-a92b-11e3-8d62-419db477a0e6_story.html.

[42] *Id.*

[43] Zoe Schiffer, *A new study from Princeton reveals how shopping websites use 'dark patterns' to trick you into buying things you didn't actually want*, BUSINESS INSIDER (Jun. 25, 2019), https://www.businessinsider.com/dark-patterns-online- shopping-princeton-2019-6.

[44] Sarah Perez, *Sneaky subscriptions are plaguing the App Store*, TECHCRUNCH (Oct. 15, 2018) https://techcrunch.com/2018/10/15/sneaky-subscriptions-are-plaguing-the-app-store.

subscription marketing plan."[45] Moreover, "the rapid growth of subscriptions has created a host of challenges for the economy, far outpacing the government's ability to combat aggressive marketing practices and ensure that consumers are being treated fairly, consumer advocates say."[46] Thus, although "Federal Trade Commission regulators are looking at ways to make it harder for companies to trap consumers into monthly subscriptions that drain their bank accounts [and] attempting to respond to a proliferation of abuses by some companies over the past few years[,]"[47] widespread utilization of these misleading "dark patterns" and deliberate omissions persist.

42. The term "dark patterns" used herein is not a science fiction reference, but a term of art from the field of user experience ("UX"). The International Organization for Standardization (ISO) defines "user experience" as a "person's perceptions and responses that result from the use or anticipated use of a product, system or service."[48] Dark patterns in UX are "carefully designed misleading interfaces by UX design experts that trick the users into choosing paths that they didn't probably want to take, thus fulfilling the business objectives, completely ignoring the requirements and ethics of users."[49]

43. The term "dark patterns" was first coined by cognitive scientist Harry Brignull, who borrowed from existing UX terminology. In UX, designers refer to common, re-usable solutions to a problem as a "design pattern," and conversely to common mistakes to solutions as "anti-

---

[45] Heather Long and Andrew Van Dam, *supra* note 35 ("'Subscription services are a sneaky wallet drain,' said Angela Myers, 29, of Pittsburgh. 'You keep signing up for things and they make it really hard to cancel.'"); *see also The problem with subscription marketing*, NEW MEDIA AND MARKETING (Mar. 17, 2019), https://www.newmediaandmarketing.com/the-problem-with-subscription-marketing.

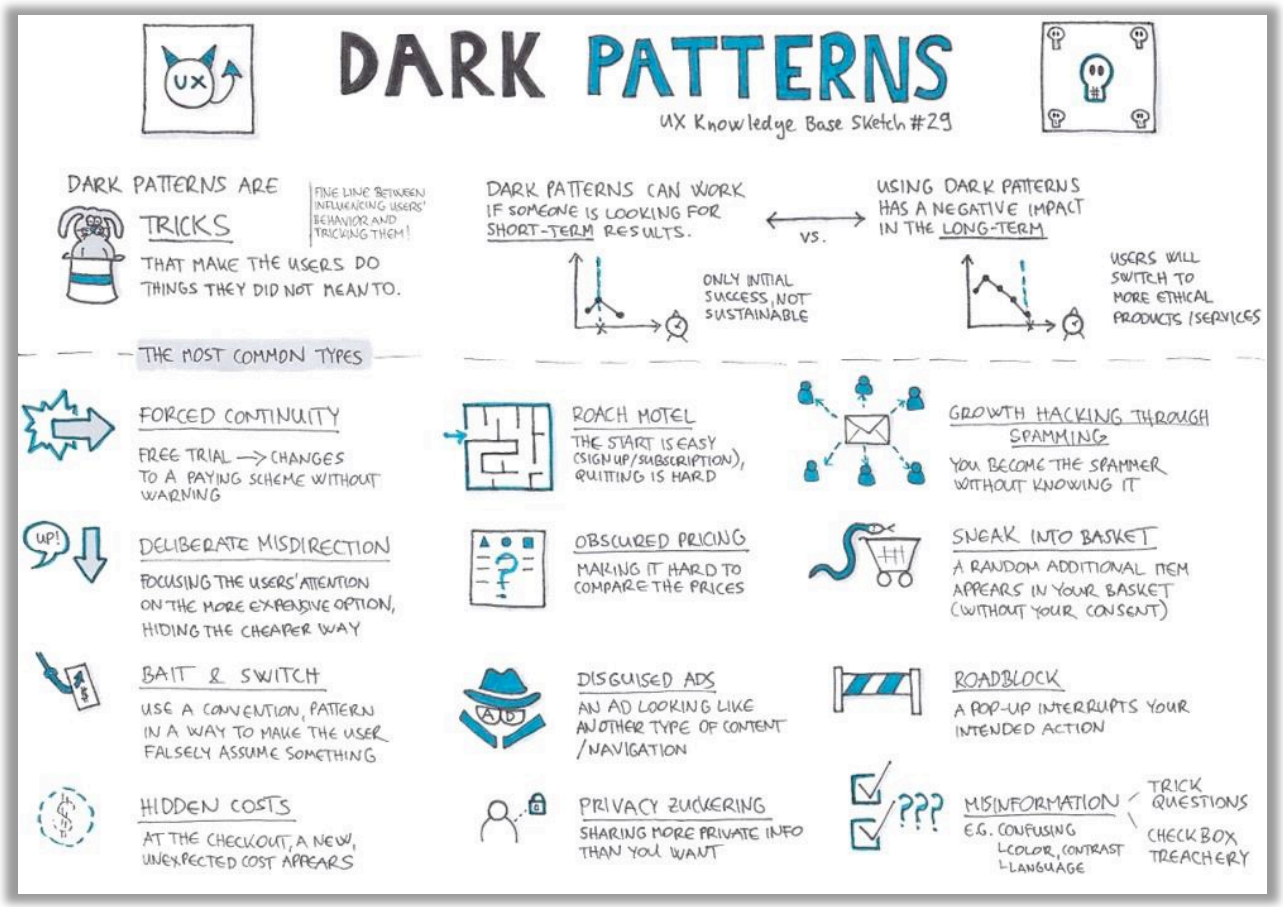
[46] *Id.*

[47] *Id.*

[48] *User Experience (UX): Process and Methodology*, UIUX TREND, https://uiuxtrend.com/user-experience-uxprocess/.

[49] Joey Ricard, *UX Dark Patterns: The Dark Side Of The UX Design*, KLIZO SOLS. PVT. LTD. (Nov. 9, 2020), https://klizos.com/ux-dark-patterns-the-dark-side-of-the-ux-design.

patterns."[50] The term "dark patterns" was intended to "communicate the unscrupulous nature" of the design "and also the fact that it can be shadowy and hard to pin down."[51] The following image provides examples of commonly employed dark patterns:[52]



44. The origin of dark patterns can be traced to the use of applied psychology and A/B testing in UX.[53] In the 1970s, behavioral science sought to understand irrational decisions and behaviors and discovered that cognitive biases guide all our thinking. The following image

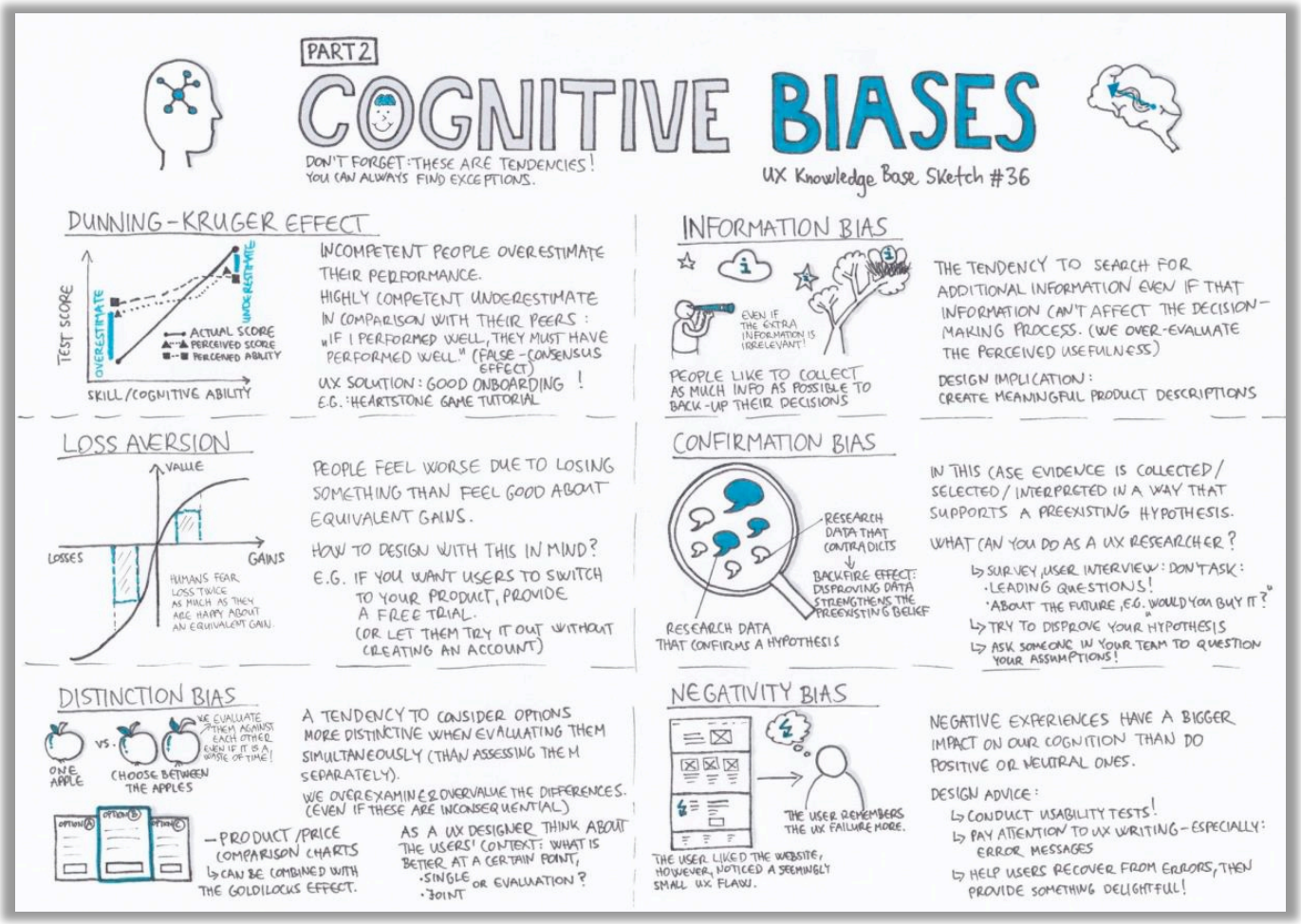
[50] Harry Brignull, *Bringing Dark Patterns to Light*, MEDIUM (Jun. 6, 2021), https://harrybr.medium.com/bringing-dark-patterns-to-light-d86f24224ebf.

[51] *Id.*

[52] Sarbashish Basu, *What is a dark pattern? How it benefits businesses- Some examples*, H2S MEDIA (Dec. 19, 2019), https://www.how2shout.com/technology/what-is-a-dark-pattern-how-it-benefit-businesses-with-some-examples.html.

[53] Brignull, *supra* note 49.

provides examples of cognitive biases, including some that Defendants employ in their cancellation process: [54]



45. But while the early behavioral research focused on understanding rather than intervention, later researchers, like Cass Sunstein and Richard Thaler (authors of the book *Nudge*) shifted focus and made the policy argument that institutions should engineer "choice architectures" in a way that uses behavioral science for the benefit of those whom they serve.[55]

[54] Krisztina Szerovay, *Cognitive Bias — Part 2*, UX KNOWLEDGE BASE (Dec. 19, 2017), https://uxknowledgebase.com/cognitive-bias-part-2-fab5b7717179.

[55] Arvind Narayanan *et al.*, *Dark Patterns: Past, Present, and Future. The evolution of tricky user interfaces*, 18 ACM QUEUE 67-91 (2002), https://queue.acm.org/detail.cfm?id=3400901.

46. Another step in the development and application of such research is the use of A/B testing in UX. A/B testing is a quantitative research method that presents an audience with two variations of a design and then measures which actions they take (or do not take) in response to each variant.[56] UX designers use this method to determine which design or content performs best with the intended user base.[57] For example, a large health care provider might A/B test whether a website visitor is more or less likely to conduct a search of its doctors if the website's search function is labelled "SEARCH" versus simply identified by a magnifying glass icon.

47. Unscrupulous UX designers have subverted the intent of the researchers who discovered cognitive biases by using these principles in ways that undermine consumers' autonomy and informed choice, and they used A/B testing to turn behavioral insights into strikingly "effective" user interfaces that deceive consumers in ways that are more profitable to the company applying them.[58] For example, dark patterns can be used to increase a company's ability to extract revenue from its users by nudging or tricking consumers to spend more money than they otherwise would, hand over more personal information, or see more ads.[59]

48. Defendants have engaged in these unlawful subscription practices with great success. In 2023, Nord Security raised $100 million from investors, with the company valued at $3 billion.[60] Nord Security's products and services have over 15 million users.

---

[56] UXPin, *A/B Testing in UX Design: When and Why It's Worth It*, https://www.uxpin.com/studio/blog/ab-testing-in-ux-design-when-and-why/.

[57] *Id.*

[58] Narayanan *et al.*, *supra* note 54.

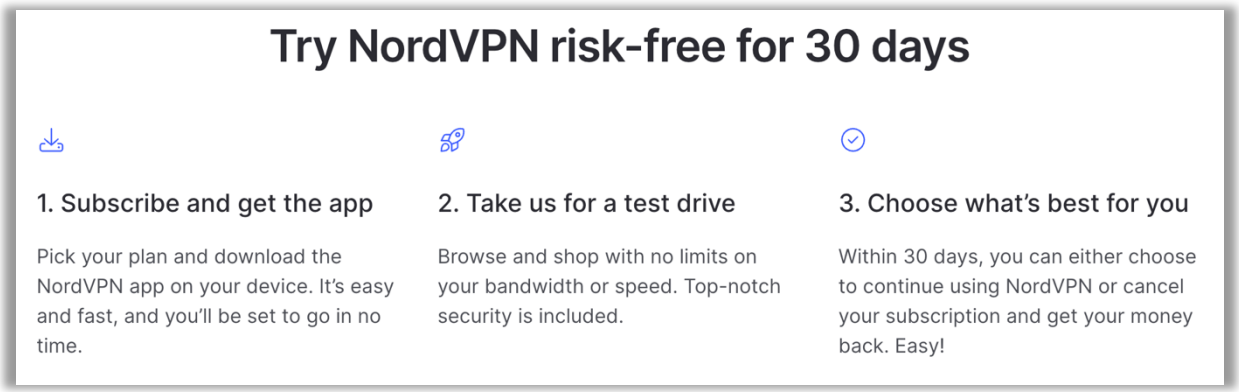
[59] *Id.*

[60] Nord Security raised another $100M investment round, NORD SECURITY, https://nordsecurity.com/blog/nord-security-raised-another-100m-investment-round.

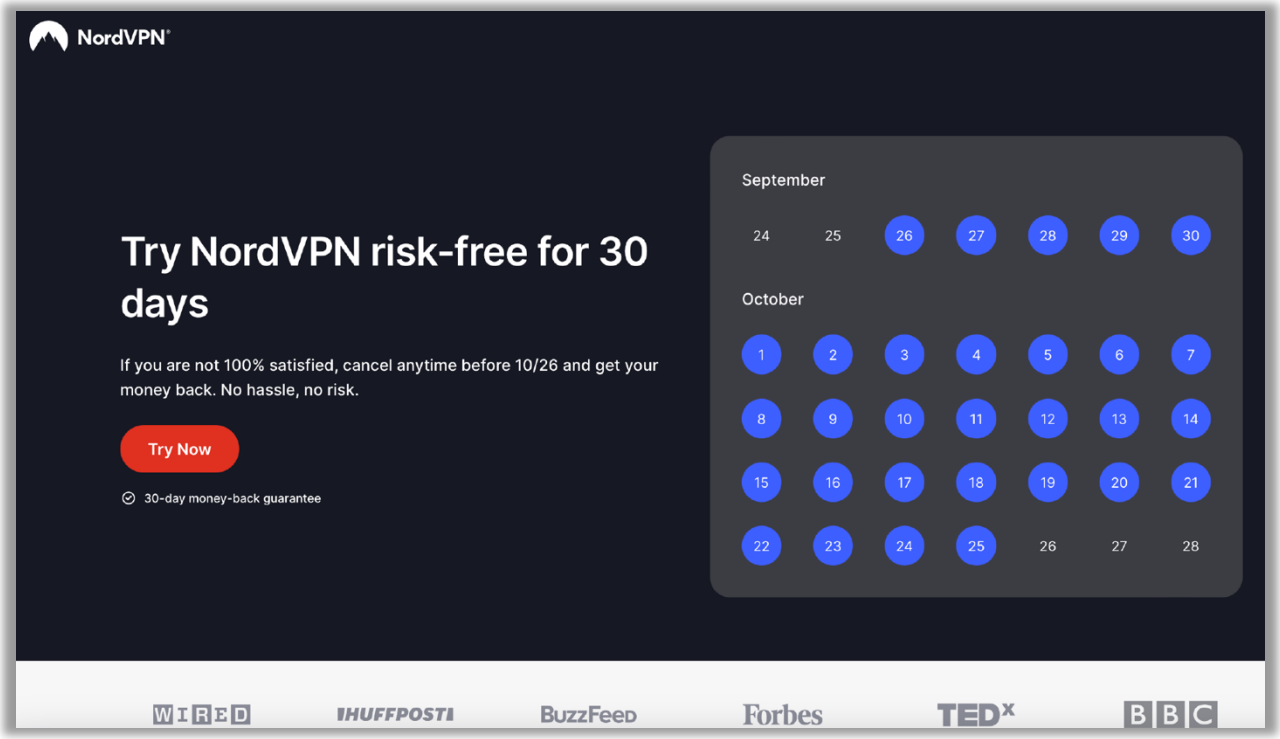
B. Nord Security's Sales Pitch and Related Material Misrepresentations and Omissions in Enrollment and Cancellation.

49. To entice consumers to become Nord Security customers, Nord Security offers consumers the opportunity to "Try NordVPN risk-free for 30 days." But rather than offer a free or reduced-price trial like many e-commerce subscription services, only charging consumers the full subscription price once the trial period ends, Nord Security employs an unusual variation of the trial model and instead charges consumers its subscriptions' full cost when the trial is initiated, but with a promise of their money back if the user cancels within the trial period.

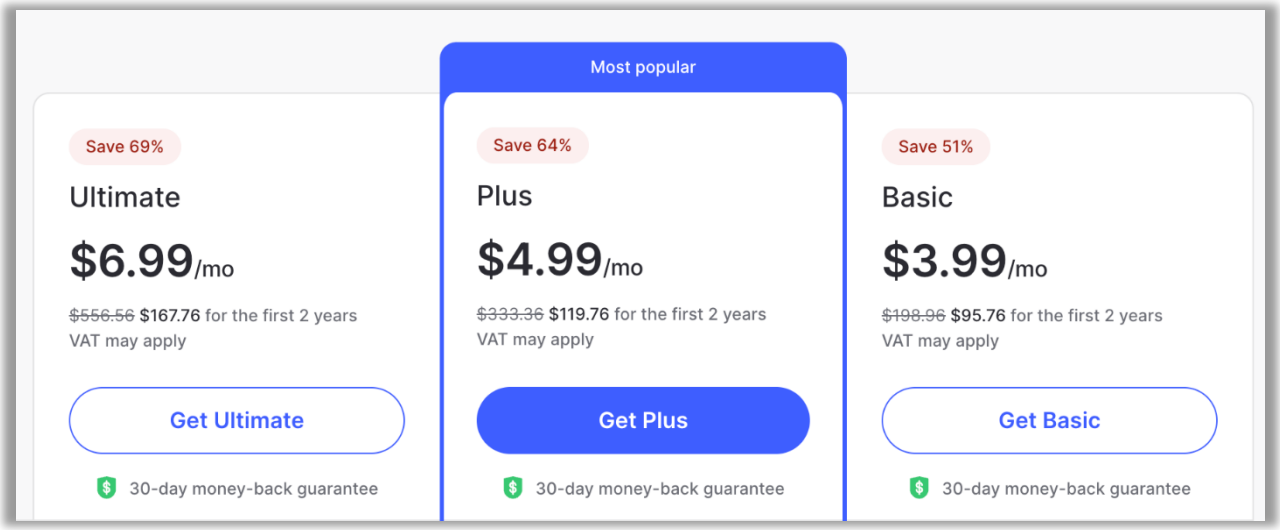
50. Indeed, Nord Security's website promises that during the 30-day trial, the consumer can "choose what's best for" them: that is, "either choose to continue using NordVPN or cancel your subscription and get your money back. Easy!" as shown in the screenshot below.



51. Nord Security further describes the trial is "no hassle, no risk," promising consumers they can "cancel anytime [in the 30-day window] and get your money back." Indeed, at the time that Plaintiff enrolled in Nord Security in August 2023, Nord Security made an offer to him that was materially similar (other than the dates) to the below screenshot captured from Nord Security's website in September 2023:

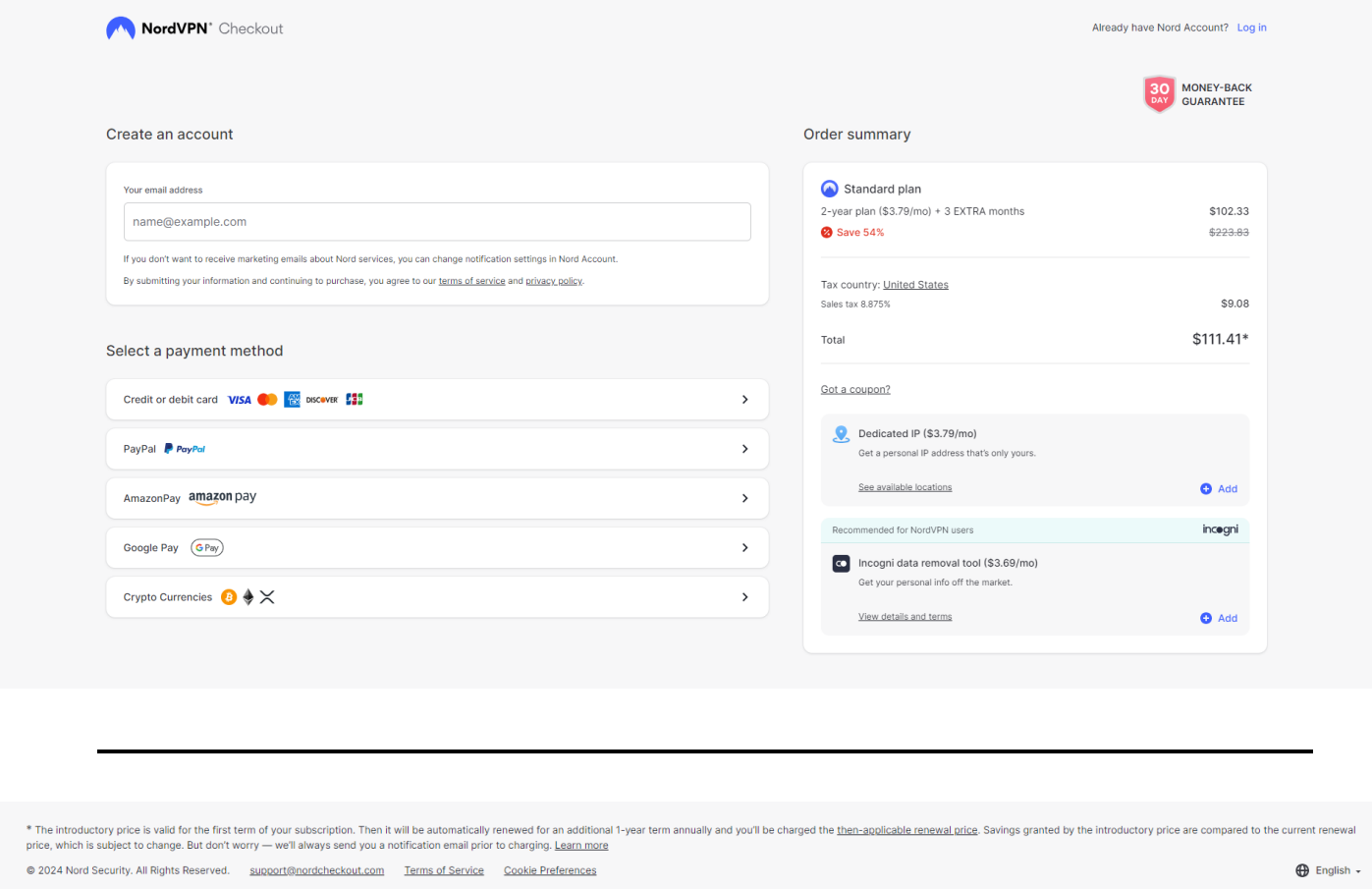


52. Indeed, upon information and belief, all Nord Security subscription plans offer this supposedly "risk-free" 30-day trial period, branding each option with its "30-day money-back guarantee" as shown in the following screenshot:



53. After a consumer elects to "try" Nord Security and selects a plan, the consumer is taken to a payment page. Upon information and belief, the payment screen for Nord Security's

enrollment process that Plaintiff used in August 2023 was materially similar to the Nord Security's payment page reproduced below, where the solid black line indicates that the user must scroll to see the rest of the page:



54. The fine print below the solid black line that includes (insufficient) autorenewal "disclosures" is on Nord Security's payment screen but is not visible unless the consumer scrolls down to view it. The terms and conditions of Nord Security's automatic renewal offer are not presented to consumers "clearly and conspicuously," as required by the North Carolina Autorenewal Law N.C.G.S. § 75-41 ("North Carolina ARL"). The automatic renewal language is not in larger type than the surrounding font. Instead, it is colored light grey rather than a more conspicuous color and is not set off from the surrounding text of the same size by symbols or other marks in a manner that clearly calls attention to the language. This violates the North Carolina

ARL. *See* N.C.G.S. § 75-41(a)(1) (requiring companies like Nord Security to "[d]isclose the automatic renewal clause clearly and conspicuously").

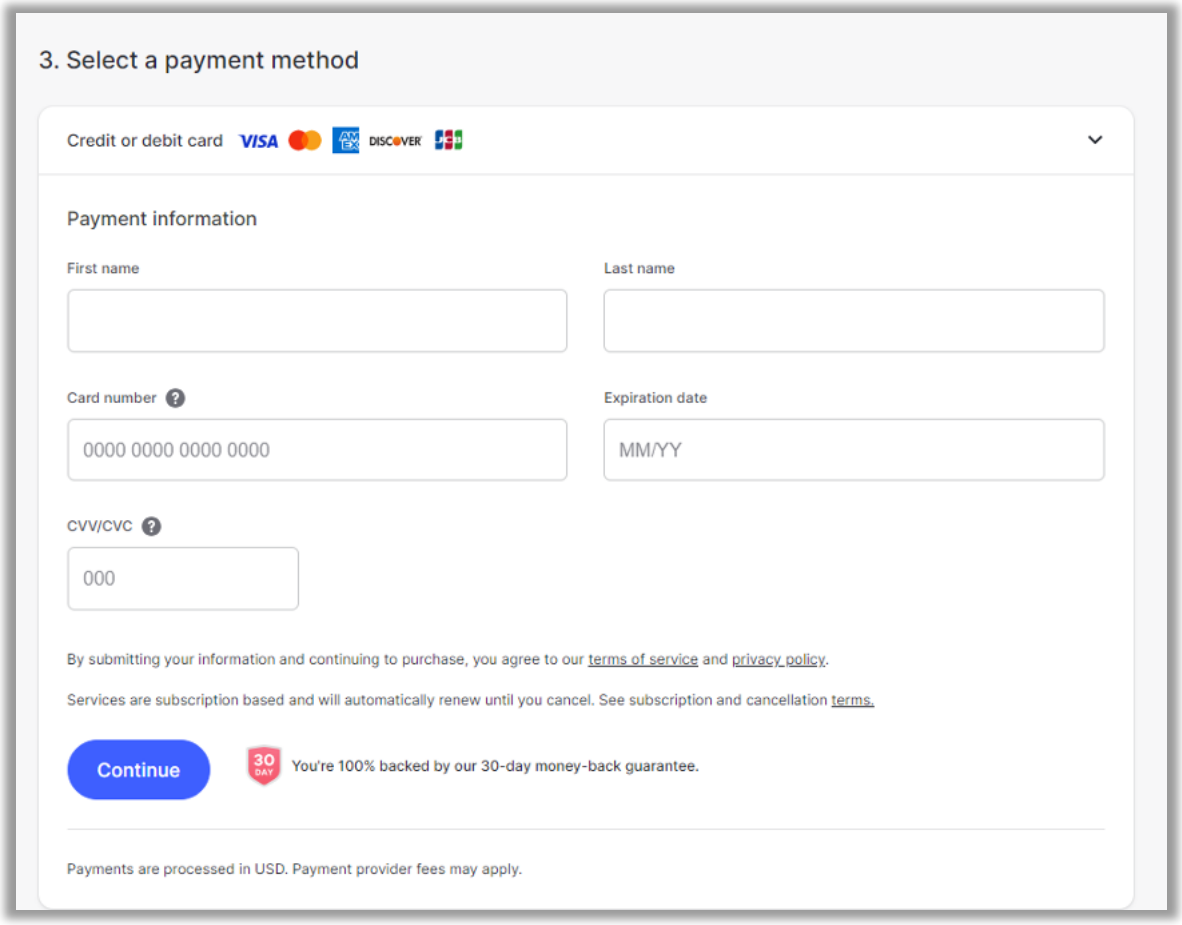
55. Instead, the payment page's overall design, including the placement of Defendants' supposed "disclosure," its font size, and color ***deemphasize*** the notice text rather than make it ***conspicuous***. Defendants' automatic renewal terms are not in visual connection with the purchase terms and are instead buried at the bottom of the page. This makes it unlikely that reasonable consumers will even see the disclosures because they must scroll down to view them, they are presented in a light grey font against a lighter gray background, and are in a single-spaced format, which makes the "disclosures" difficult to read.

56. Defendants' fine print also fails to disclose key details about Nord Security's subscription practices, including the cancellation policy, information on how to cancel, and that cancellation during the trial period is insufficient to trigger the promised refund.

57. Moreover, any supposed "disclosures" on the Nord Security payment page are far overshadowed by the page's other components in a clear demonstration of the "Misinformation" dark pattern. The payment page uses at least 12 different colors, presents information in differently sized fonts and in various boxes, and includes hyperlinks, drop-down menus styled as hyperlinks, two call-outs for add-on products, and 13 different logos. In contrast, the automatic renewal terms are hidden at the bottom of the page, difficult to discern, and easy to miss especially since consumers must scroll down on the screen to view them.

58. Nord Security's "Order Summary" box likewise does not sufficiently present the terms and conditions of its automatic renewal offer to consumers, nor does it present the consumer with an easily accessible disclosure of the methods that the consumer may use to cancel the subscription.

59. When a consumer selects a payment method on the payment screen (e.g., credit card, PayPal), the payment method box expands, again failing disclose Nord Security's autorenewal terms, let alone do so in a clear and conspicuous manner. The expanded payment boxes also do not present the consumer with any disclosure of the cancellation policy or the methods that may be used to cancel the subscription, let alone a method that is easily accessible. What the expanded payment box does do, however, is emphasize the 30-day trial period with a colorful logo placed prominently right next to the blue "Continue" button that a consumer must click after entering their payment information:



60. In sum, the Nord Security payment page fails to obtain consumers' affirmative consent to the automatic renewal terms and contains no mechanism for affirmatively consenting

to the automatic renewal terms. For example, there is no checkbox that consumers must click to indicate that they accept those terms.

61. And nowhere on the payment page does Nord Security disclose that cancellation during the trial period does not automatically initiate a refund of the consumer's upfront payment as was previously promised. Nor does Nord Security disclose critical information on this payment page, such as how to cancel, how to turn off autorenewal, by when the consumer must cancel the trial to receive a refund, or how or when to request a refund if the user decides not to become a full-fledged subscriber after the trial.

62. Instead, Nord Security provides tiny, inconspicuous hyperlinks to "terms of service" and "terms" which themselves do not clearly and conspicuously explain the nature of Nord Security's trial and promised refund, autorenewal charges, or its cancellation mechanism. Instead Nord Security scatters confusing, inconsistent, and inaccurate provisions addressing these and other issues across multiple sections of these documents (which total more than 9,500 words), burying them inconspicuously in dense surrounding text.

63. For example, upon information and belief the then-most recent versions of Nord Security's fine print documents at the time Plaintiff enrolled in his Nord Security trial twice define "cancel your Subscription" as "turn off auto-renewals for the upcoming Service period." This definition of "cancel" leaves a reasonable consumer—who had previously been told he could "cancel anytime" during the trial in order to get a refund—to understand that turning off auto-renewal was all that was necessary. True, another part of Defendants' fine print states that a consumer "may cancel the Subscription and request a refund within thirty (30) days." But that fine print does not undo Nord Security's other misrepresentations and omissions, particularly because Nord Security provides no instructions for lodging such a "request."

64. As another example, upon information and belief the then-most recent version of Nord Security's "terms of service" at the time Plaintiff enrolled in his Nord Security trial contain a paragraph labeled "Auto-Renewal," which reads as follows:

> 3.2 **Auto-Renewal**. After the end of your Service period, your Subscription will automatically renew for the successive defined Service periods at the renewal dates, unless you decide to cancel the Subscription renewal before the day of the charge. If you do not cancel the Subscription in such due course, your chosen payment method will be charged the then-current renewal price for the upcoming defined Service period.

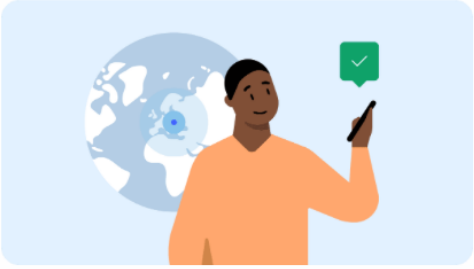
65. This "Auto-Renewal" paragraph gives reasonable consumers the impression that they will be charged only ***after*** the original subscription ends. Meanwhile, the separate "terms" document reveals, in a paragraph not cross referenced in the "Auto-Renewal" paragraph above, that customers on plans lasting greater than a month will be charged in advance: "at least 14 days before" the scheduled auto-renewal. This provision is itself in conflict with another "provision in the same "terms" document, which provides that "***[a]fter the end*** of your initial plan, your subscription ***will be automatically renewed***, and you will ***be charged***[.]" (emphasis added). In other words, this paragraph in the "terms" document expressly states that the consumer will ***not*** be charged until "after" the subscription period ends, not "at least fourteen days" before.

66. After Plaintiff enrolled in Nord Security, Nord Security sent Plaintiff an email with the subject line "Welcome to NordVPN!" A representative version of the acknowledgement email sent to Plaintiff and other consumers is shown on the following page:

NordVPN

Connect to NordVPN and encrypt your traffic

Welcome to the world of privacy and security!
You're all set to use NordVPN.



Connect now to reduce everyday online risks and make sure you browse the web safely.

Connect Now

Don't leave gaps in your security. Explore all features and benefits NordVPN has to offer.

Protect all your devices
You can use NordVPN on 6 devices at the same time. Find NordVPN apps for all devices here.

Fend off cyber threats
Block web trackers, ads, and malicious websites and files with the Threat Protection feature for desktop apps. Turn on.

Check if your data has leaked
Scan the dark web for login details associated with your email address with Dark Web Monitor feature. Check now.

If you're in a country that restricts VPNs, click here.

Stay safe!
The NordVPN team

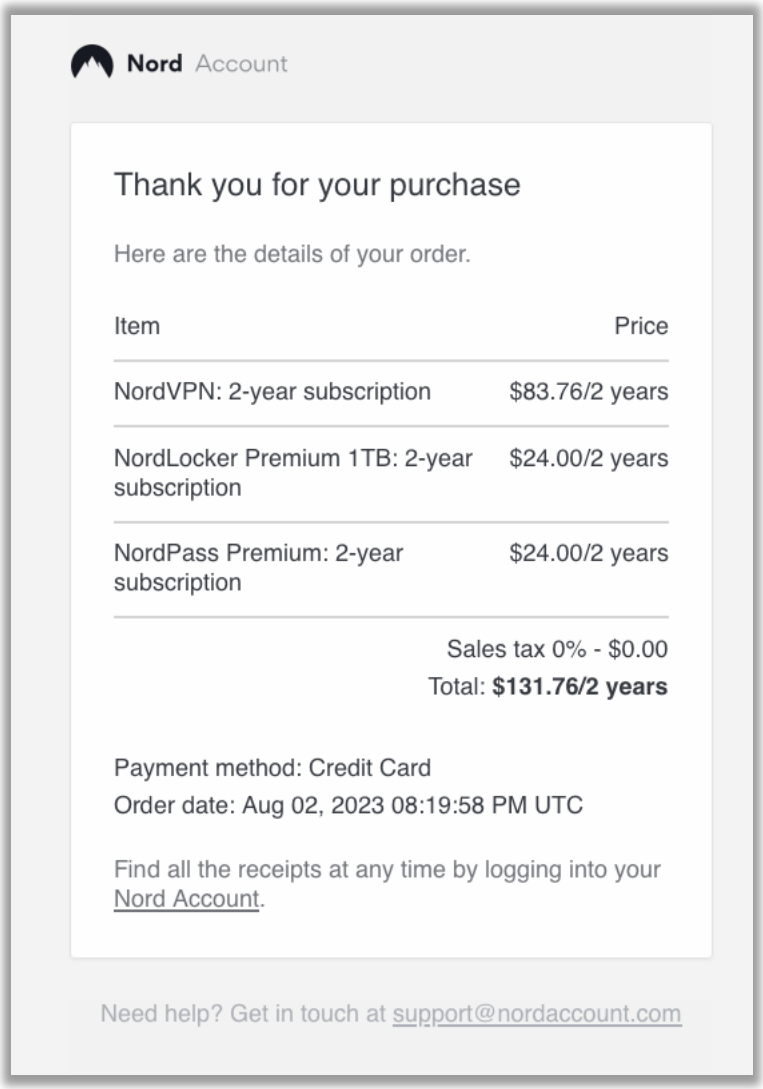
Earn 3 free months - refer your friends
Invite your friends to use NordVPN and get rewards.

Earn 3 Free Months

Get the app | Need help?

PH F&F TOWER, 50th Street & 56th Street, Suite #32-D, Floor 32, Panama City, Republic of Panama

67. After Plaintiff enrolled in Nord Security, Nord Security also sent Plaintiff an email containing the word "receipt" in the subject line. The content of the email sent to Plaintiff is shown below:



Nord Account

Thank you for your purchase

Here are the details of your order.

Item	Price
NordVPN: 2-year subscription	$83.76/2 years
NordLocker Premium 1TB: 2-year subscription	$24.00/2 years
NordPass Premium: 2-year subscription	$24.00/2 years

Sales tax 0% - $0.00

Total: **$131.76/2 years**

Payment method: Credit Card

Order date: Aug 02, 2023 08:19:58 PM UTC

Find all the receipts at any time by logging into your Nord Account.

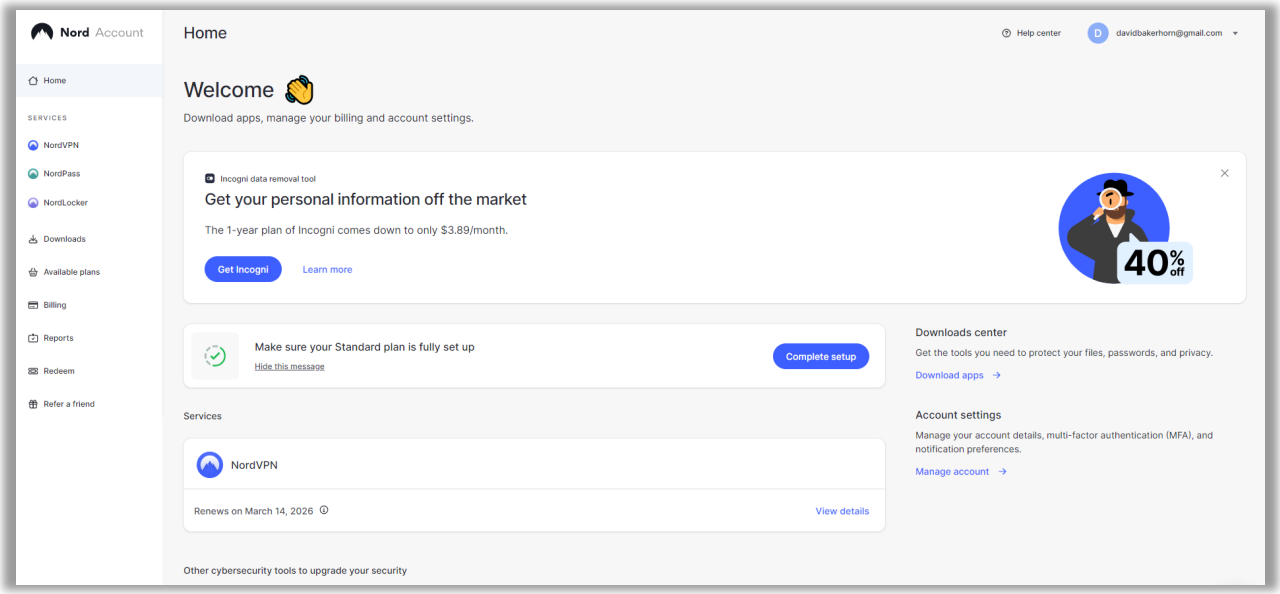
Need help? Get in touch at support@nordaccount.com

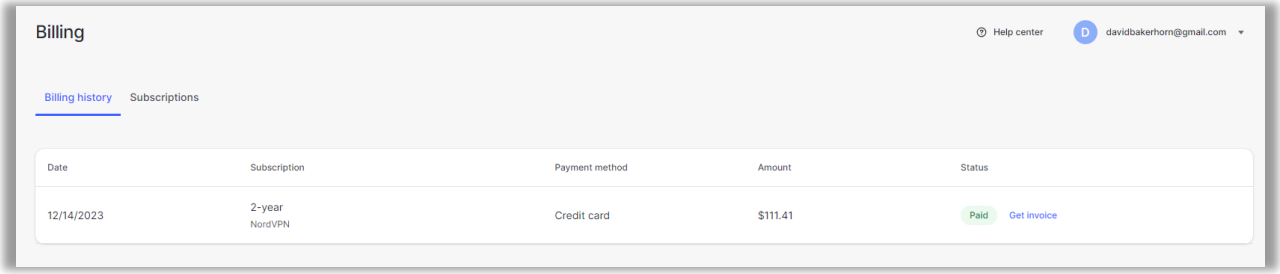
68. Neither Defendants' acknowledgement nor receipt emails meet the post-purchase requirements that the North Carolina ARL imposes on an automatically renewing product or service, nor do they provide any information on Nord Security's cancellation policy, let alone disclose "clearly and conspicuously how to cancel the contract." N.C.G.S. § 75-41(a)(2). In fact, neither of these emails include any disclosure whatsoever about how to cancel a Nord Security account or obtain a refund.

C. Nord Security's Cancellation Process is Unfair and Deceptive

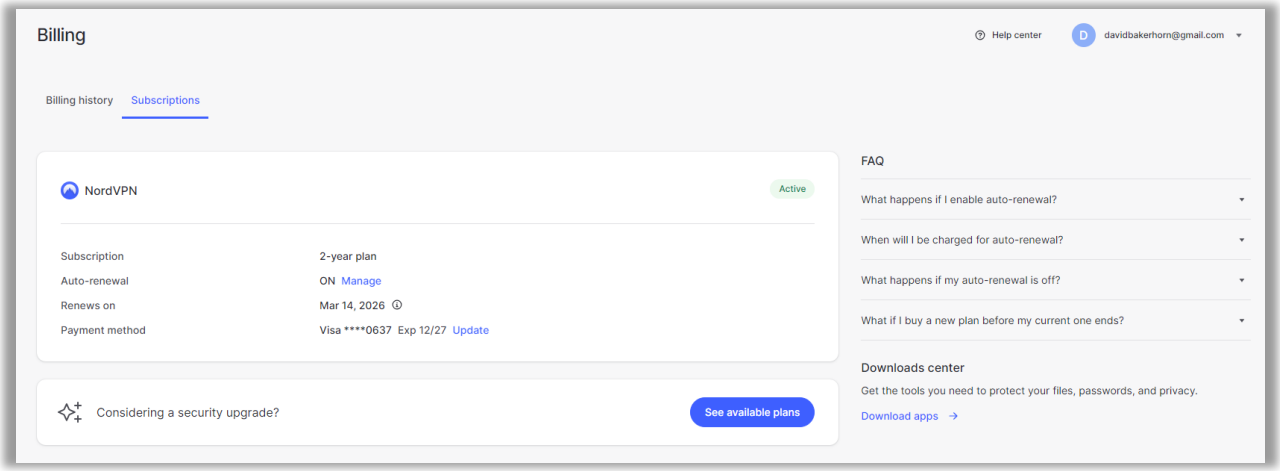
69. Nord Security's cancellation process is not simple, cost-effective, timely, easy-to-use, nor readily accessible to consumers. Instead, Nord Security employs the "roach motel" strategy: it is easy to sign up for Nord Security products and services, but hard to get out.

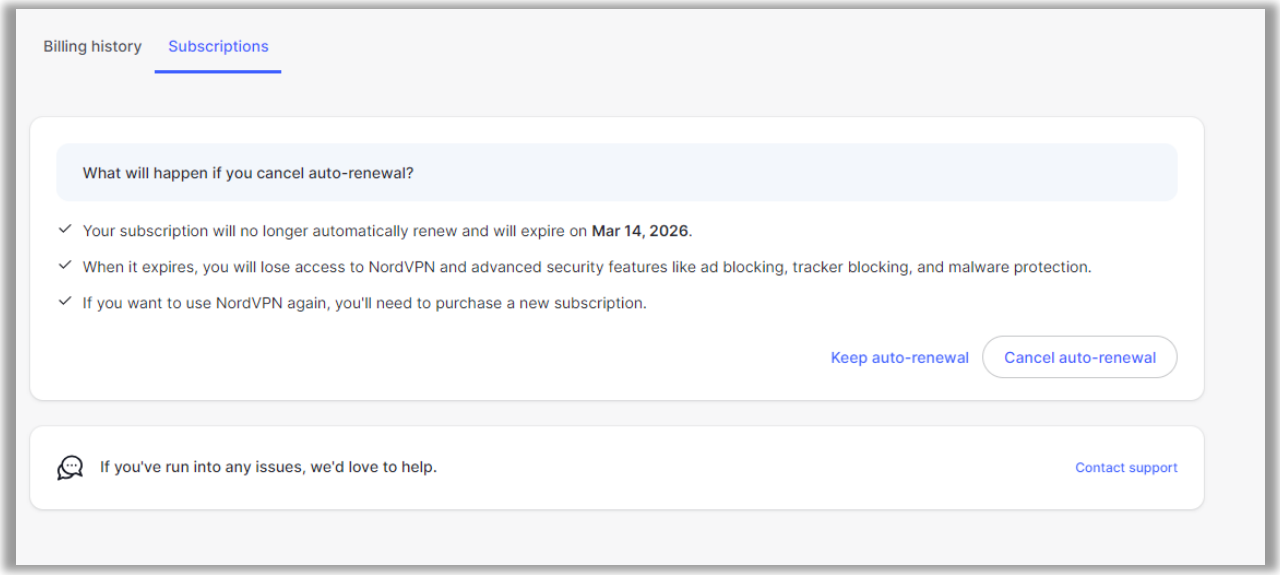
70. Nord Security buries its cancellation mechanism four layers deep in its customer account portal, with no clear path evident to the consumer for how to get there. Canceling a Nord Security subscription first requires consumers to (1) log into their customer account, and (2) select "Billing" from a list of at least nine options. Once "Billing" is selected, the default view on the "Billing" page does not mention anything about cancellation, and instead shows the consumer's "Billing history." Upon information and belief, Nord Security's "Home" and "Billing" pages available to Plaintiff in or around August 2023 were materially similar to Nord Security's current Home and Billing pages copied below and on the next page:





71. After navigating to Nord Security's "Billing page," consumers wishing to cancel must then (3) figure out how to navigate to the "Subscriptions" tab on the "Billing" page. Once customers access the "Subscriptions" tab, they are still not presented with a "Cancel" option. Instead, consumers must then (4) understand that they need to click on "Manage" on a line pertaining to "Auto-renewal" to finally access a page where they can cancel their account. Upon information and belief, Nord Security's "Subscriptions" tab available to Plaintiff in or around August 2023 was materially similar to the Nord Security "Subscriptions" tab as copied below, as well as the page consumers view when they click "Manage" next to "Auto-renewal," in the image on the next page:





72. For consumers who manage to find and click "Cancel auto-renewal," the autorenewal is finally canceled. But Nord Security's multi-step cancellation process is specifically and intentionally designed to thwart cancellation—a "roach motel" dark pattern that prevents consumers from finding and canceling autorenewal. This is an unfair and deceptive trade practice that violates North Carolina's consumer protection statute. *See* N.C.G.S. § 75-1.1(a).

D. Nord Security misrepresented and failed to clearly and conspicuously disclose the terms of its 30-day trial

73. Nord Security represented that it offered a 30-day trial with a money-back refund guarantee that would allow consumers to "Try NordVPN risk-free for 30 days" and "get your money back. No hassle, no risk" if the consumer cancelled within 30 days of sign up.

74. Nord Security deceived consumers into believing that if they were not satisfied with Nord Security's offerings, they would receive a refund simply by "cancel[ing] anytime" within that 30-day period.

75. But rather than refund consumers who cancelled within the specified trial period, Nord Security in fact required consumers to both cancel the subscription ***and*** request a refund

within the 30-day period. Nord Security did not adequately disclose that cancellation within 30 days of sign up was insufficient to trigger a refund of the consumer's initial payment.

76. Nord Security also placed a further limitation on the trial offer, allowing consumers to get a refund only if they had not received a refund from Nord Security more than two times before. Nord Security also did not clearly and conspicuously disclose this limitation on their refund policy in their online marketing.

E. How Nord Security's Subscription Practices Injured Plaintiff

77. Plaintiff was injured by Nord Security's unlawful and deceptive subscription practices because had Plaintiff known that Nord Security's trial was not actually a "risk-free" 30-day trial that would allow him to get his money back simply by "cancel[ing] anytime" during the trial period, he would not have enrolled in a Nord Security subscription.

78. On approximately August 2, 2023, Plaintiff enrolled in a 30-day trial of Nord Security's NordVPN, NordLocker, and NordPass services.

79. On August 2, 2023, Nord Security charged $131.76 to Plaintiff's credit card. The same day, Plaintiff received a receipt from Nord Security for $83.76 for the VPN service, $24.00 for NordLocker, and $24.00 for NordPass, for a total of $131.76.

80. After signing up to "try" Defendants' services, Plaintiff downloaded the NordVPN app. Plaintiff accessed his Nord Security offerings a few times during the trial period, but decided he did not want to continue.

81. On August 15, 2023, Plaintiff contacted Nord Security customer service and directed the Company to cancel his Nord Security subscriptions. Nord Security then informed Plaintiff that his subscription had been cancelled and he would not be charged unless he resubscribed to Nord Security.

82. Later on August 15, 2023, Plaintiff received an email from Nord Security advising that the automatic renewal feature of his subscription had been cancelled.

83. Having decided not to become a full-fledged Nord Security subscriber, and having communicated this to the Company, Plaintiff believed that once the trial period was over, he would no longer be a Nord Security customer and that he would get his money back. Plaintiff had canceled his Nord Security subscriptions before the 30-day trial period ended.

84. Nord Security did not adequately disclose to Plaintiff that it would retain his $131.76 payment despite his cancellation during the 30-day trial unless he affirmatively requested a refund. Plaintiff reasonably believed that, consistent with Nord Security's promise that he could "cancel anytime [during the 30-day period] and get [his] money back," he would in fact be refunded upon timely cancellation.

85. On approximately September 26, 2023, Plaintiff saw on a third-party billing statement that Nord Security had not refunded him any of $131.76 that he was charged on or around August 2, 2023.

86. When Plaintiff contacted Nord Security customer service about the expected refund, he was told that he had only canceled the autorenewal that was set to occur ***after*** a two-year subscription expired and not the trial, despite the "no risk" trial guarantee. Nord Security's customer service refused to give Plaintiff a refund.

87. After Nord Security refused to issue Plaintiff a refund, he contacted his credit card company to dispute the charge. The credit card company sided with Plaintiff and issued a temporary credit to his account on September 26, 2023. Shortly thereafter, on September 28, 2023, Nord Security reversed course and issued a refund, after which the credit card company removed the temporary credit.

88. Nord Security did not "clearly and conspicuously" disclose to Plaintiff how he could cancel his Nord Security subscriptions during the (supposedly "risk-free") 30-day trial and obtain the promised full refund. This information is not clearly and conspicuously provided in the contract offers made on Nord Security's website, in any hyperlinked terms on the website, or in any post-purchase acknowledgment or receipt email.

89. Plaintiff did not authorize or want his Nord Security subscriptions to continue beyond the 30-day trial period. In fact, Plaintiff affirmatively canceled his subscriptions before the trial ended, but Nord Security kept his initial payment for a full subscription term anyway, despite its promise of a full refund upon cancellation.

90. Plaintiff was injured when Nord Security failed to refund its prior charge of $131.76 to his credit card after Plaintiff cancelled his subscriptions during the trial period, despite inducing him to sign up with its promise to refund him should he cancel during the trial, and instead left him with Nord Security subscriptions he did not want and did not want to pay for.

91. Nord Security wrongfully retained Plaintiff's funds from August 15, 2023 until September 28, 2023. During that time, Plaintiff was unable to use those funds. Plaintiff was further damaged by the lost time value of his funds between August 15, 2023 and September 28, 2023.

92. Plaintiff was further injured by Nord Security's subscription practices because had he known the truth about Nord Security's intentionally misleading trial period and subscription practices, he would not have enrolled in Nord Security.

93. Plaintiff intends to purchase products and services in the future for himself from internet security companies, including Nord Security, as long as he can gain some confidence in Nord Security's representations about its products and services and trial and subscription practices,

including autorenewal and cancellation. Moreover, Nord Security still has Plaintiff's payment information and could use it to process unauthorized payments in the future.

CLASS ACTION ALLEGATIONS

94. Plaintiff brings this action on his own behalf and additionally, pursuant to Rule 23(b)(2) and (3) of the Federal Rules of Civil Procedure, on behalf of a class of all Nord Security customers in the United States who were subjected to Defendants' misleading subscription practices from the earliest allowable date through the date of judgment (the "Class").

95. Plaintiff also brings this action on his own behalf and additionally, pursuant to Rule 23(b)(2) and (b)(3) of the Federal Rules of Civil Procedure, on behalf of a class of all Nord Security customers in the state of [*e.g.*, North Carolina] (including customers of companies Nord Security acts as a successor to) who were automatically enrolled into and charged for at least one month of Nord Security membership by Defendants at any time from [applicable statute of limitations period] to the date of judgment (the "Subclasses").

96. As alleged throughout this Complaint, the Class claims all derive directly from a single course of conduct by Defendants. Defendants have engaged in uniform and standardized conduct toward the Class and this case is about the responsibility of Defendants, at law and in equity, for their knowledge and conduct in deceiving their customers. Defendants' conduct did not meaningfully differ among individual Class Members in their degree of care or candor, their actions or inactions, or in their false and misleading statements or omissions. The objective facts on these subjects are the same for all Class Members.

97. Excluded from the Class are: Defendants; any parent, subsidiary, or affiliate of Defendants; any entity in which Defendants have or had a controlling interest, or which Defendants otherwise control or controlled; and any officer, director, employee, legal representative, predecessor, successor, or assignee of Defendants. Also excluded are federal, state and local

government entities; and any judge, justice, or judicial officer presiding over this action and the members of their immediate families and judicial staff.

98. Plaintiff reserves the right, as might be necessary or appropriate, to modify or amend the definition of the Class and/or add Subclasses, when Plaintiff files his motion for class certification.

99. Plaintiff does not know the exact size of the Class since such information is in the exclusive control of Defendants. Plaintiff believes, however, that the Class encompasses thousands of consumers whose identities can be readily ascertained from Nord Security's records. Accordingly, the members of the Class are so numerous that joinder of all such persons is impracticable.

100. The Class is ascertainable because its members can be readily identified using data and information kept by Defendants in the usual course of business and within their control. Plaintiff anticipates providing appropriate notice to each Class Member in compliance with all applicable federal rules.

101. Plaintiff is an adequate class representative. Plaintiff's claims are typical of the claims of the Class and do not conflict with the interests of any other members of the Class. Plaintiff and the other members of the Class were subject to the same or similar conduct engineered by Defendants. Further, Plaintiff and members of the Class sustained substantially the same injuries and damages arising out of Defendants' conduct.

102. Plaintiff will fairly and adequately protect the interests of all Class Members. Plaintiff has retained competent and experienced class action attorneys to represent his interests and those of the Class.

103. Questions of law and fact are common to the Class and predominate over any questions affecting only individual Class members, and a class action will generate common answers to the questions below, which are apt to drive the resolution of this action:

a. Whether Defendants' conduct violates the North Carolina ARL;

b. Whether Defendants' conduct violates the applicable North Carolina consumer protection statutes;

c. Whether Defendants were unjustly enriched as a result of their conduct;

d. Whether Class Members have been injured by Defendants' conduct;

e. Whether, and to what extent, equitable relief should be imposed on Defendants to prevent them from continuing their unlawful practices; and

f. The extent of class-wide injury and the measure of damages for those injuries.

104. A class action is superior to all other available methods for resolving this controversy because (1) the prosecution of separate actions by Class Members will create a risk of adjudications with respect to individual Class Members that will, as a practical matter, be dispositive of the interests of the other Class Members not parties to this action, or substantially impair or impede their ability to protect their interests; (2) the prosecution of separate actions by Class Members will create a risk of inconsistent or varying adjudications with respect to individual Class Members, which will establish incompatible standards for Defendants' conduct; (3) Defendants have acted or refused to act on grounds generally applicable to all Class Members; and (4) questions of law and fact common to the Class predominate over any questions affecting only individual Class Members.

105. Further, the following issues are also appropriately resolved on a class-wide basis under Federal Rule of Civil Procedure 23(c)(4):

a. Whether Defendants' conduct violates the ARL;

b. Whether Defendants' conduct violates the applicable North Carolina consumer protection statutes;

c. Whether Defendants were unjustly enriched as a result of their conduct;

d. Whether Class Members have been injured by Defendants' conduct;

e. Whether, and to what extent, equitable relief should be imposed on Defendants to prevent them from continuing their unlawful practices; and

f. The extent of class-wide injury and the measure of damages for those injuries.

106. Accordingly, this action satisfies the requirements set forth under Rules 23(a), (b)(2), (b)(3), and (c)(4) of the Federal Rule of Civil Procedure.

COUNT I

NORTH CAROLINA AUTOMATIC RENEWAL LAW (N.C.G.S. § 75-41, *et seq.*)
(ON BEHALF OF THE NORTH CAROLINA CLASS
UNDER NORTH CAROLINA LAW)

107. Plaintiff incorporates by reference all preceding and subsequent paragraphs.

108. Plaintiff brings this claim on his own behalf and on behalf of each member of the North Carolina Class.

109. Plaintiff signed up for a 30-day trial subscription of Nord Security services that would automatically renew as a full subscription at the end of the trial period absent successful cancellation.

110. The North Carolina ARL requires that any person offering a contract that "automatically renews unless the consumer cancels the contract" must disclose: (1) "the automatic renewal clause clearly and conspicuously in the contract or contract offer," and (2) clearly and conspicuously how to cancel the contract in the initial contract, contract offer, or with delivery of products or services." N.C.G.S. §§ 75-41(a)(1)–(2). Defendants' failure to comply includes at least the following independent violations:

a. Nord Security failed to clearly and conspicuously disclose the automatic renewal clause in its subscription offer and fine print terms, as required by N.C.G.S. § 75-41(a)(1); and

b. Nord Security failed to clearly and conspicuously disclose how to cancel the contract in the initial contract, contract offer, or with delivery of products or services, as required by N.C.G.S. § 75-41(a)(2), including by failing to disclose how to "cancel anytime . . . and get your money back" within the 30-day trial period that accompanies every Nord Security subscription plan.

111. Defendants' violations of the North Carolina ARL "renders the automatic renewal clause void and unenforceable." N.C.G.S. § 75-41(e).

112. Defendants are not afforded any of the protections of N.C.G.S. §75-41(c) as, upon information and belief, Defendants cannot demonstrate that they: (1) have established and implemented written procedures to comply with N.C.G.S. §75-41 and enforce compliance with the procedures; (2) any failure to comply with N.C.G.S. § 75-41 is the result of error; and (3) where an error has caused the failure to comply with N.C.G.S. § 75-41, Defendants provide full refunds or credit for all amounts billed or paid by Plaintiff and Class members from the date of the renewal until the date of the termination of the contract, or the date of the subsequent notice of renewal, whichever occurs first.

113. Plaintiff and the North Carolina Class Members suffered monetary damages as a result of Defendants' conduct.

114. Defendants are liable to Plaintiff and the North Carolina Class Members for actual damages sustained.

COUNT II

NORTH CAROLINA UNFAIR AND DECEPTIVE TRADE PRACTICES ACT (N.C.G.S. § 75-1.1, *et seq.*) (ON BEHALF OF THE NORTH CAROLINA CLASS AGAINST DEFENDANTS)

115. Plaintiff incorporates by reference all preceding and subsequent paragraphs.

116. Plaintiff brings this claim on his own behalf and on behalf of each member of the North Carolina Class.

117. North Carolina's Unfair and Deceptive Trade Practices Act, N.C.G.S. § 75-1.1, *et seq*. ("NCUDTPA"), prohibits a person from engaging in "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce[.]" The NCUDTPA provides a private right of action for any person injured "by reason of any act or thing done by any other person, firm or corporation in violation of" the NCUDTPA. N.C.G.S. § 75-16.

118. Defendants engaged in unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, with respect to the sale and advertisement of the products and services purchased by Plaintiff and the North Carolina Class Members, in violation of N.C.G.S. § 75-1.1(a), including by making false representations or concealing the true risks of a Nord Security trial or subscription, and by failing to engage in fair and upright business practices.

119. The above unfair or deceptive acts or practices by Defendants were conducted in or affecting "commerce," as defined by N.C.G.S. § 75-1.1(b).

120. The above unfair or deceptive acts or practices by Defendants were reasonably and intentionally calculated to deceive class members and other consumers.

121. The above unfair or deceptive acts or practices by Defendants did in fact deceive class members and other consumers, causing them damage.

122. The above unfair and deceptive practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous.

123. Defendants' actions were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and the North Carolina Class Members.

124. Plaintiff and the North Carolina Class Members relied on Defendants' representations in that they would not have purchased, chosen, and/or paid for all or part of Nord Security's products and services had they known the truth about the risks of subscribing to Nord Security, including the risks of its 30-day trial period.

125. As a direct and proximate result of Defendants' deceptive acts and practices, Plaintiff and the North Carolina Class Members suffered an ascertainable loss of money or property, real or personal, as described above.

126. Plaintiff and the North Carolina Class Members seek relief under N.C.G.S. §§ 75-16 and 75-16.1, including, but not limited to injunctive relief, damages, treble damages, and attorneys' fees and costs.

COUNT III

CONVERSION

(ON BEHALF OF A MULTISTATE CLASS UNDER NORTH CAROLINA LAW OR, ALTERNATIVELY, THE LAWS OF EACH STATE WHERE DEFENDANTS DO BUSINESS OR, ALTERNATIVELY, ON BEHALF OF EACH INDIVIDUAL STATE CLASS)

127. Plaintiff incorporates by reference all preceding and subsequent paragraphs.

128. Plaintiff brings this claim on his own behalf and on behalf of each member of the Multistate Class under North Carolina law or under the laws of each of the states where Defendants do business that permit an independent cause of action for conversion, or, alternatively, on behalf of each member of the individual State Classes under the laws of those States.

129. In all states where Defendants do business, there is no material difference in the law of conversion as applied to the claims and questions in this case.

130. Plaintiff and the Class own and have a right to possess the money that is in their respective bank accounts, internet payment accounts, and/or credit cards.

131. Defendants substantially interfered with Plaintiff and the Class's possession of this money by knowingly and intentionally making unauthorized charges to their bank accounts, internet payment accounts, and/or credit cards for Nord Security subscriptions and/or failing provide refunds for consumers who cancelled their subscriptions during Nord Security's 30-day trial period.

132. Plaintiff and the Class never consented to Defendants taking of this money from their bank accounts, internet payment accounts, and/or credit cards and/or to Defendants maintaining possession of money that should have been returned to Plaintiff and Class upon cancellation during Nord Security's 30-day trial.

133. Defendants wrongfully retained dominion over this monetary property and/or the time-value of the monetary property.

134. Plaintiff and the Class have been damaged by Defendants' wrongful taking and/or possession of such money from their bank accounts, internet payment accounts, and/or credit cards in an amount that is capable of identification through Defendants' records.

135. By reason of the foregoing, Defendants are liable to Plaintiff and the Class for conversion in an amount to be proved at trial.

COUNT IV

UNJUST ENRICHMENT

(ON BEHALF OF A MULTISTATE CLASS UNDER NORTH CAROLINA LAW OR, ALTERNATIVELY, THE LAWS OF EACH STATE WHERE DEFENDANTS DO BUSINESS OR, ALTERNATIVELY, ON BEHALF OF EACH INDIVIDUAL STATE CLASS)

136. Plaintiff incorporates by reference all preceding and subsequent paragraphs.

137. Plaintiff brings this claim on his own behalf and on behalf of each member of the Multistate Class under North Carolina law or the laws of each of the states where Defendants do

business that permit an independent cause of action for unjust enrichment, or, alternatively, on behalf of each member of the individual State Classes under the laws of those States.

138. In all states where Defendants do business, there is no material difference in the law of unjust enrichment as applied to the claims and questions in this case.

139. As a result of their unjust conduct, Defendants have been unjustly enriched.

140. As a result of Defendants violations of the North Carolina ARL, Nord Security's automatic renewal clause is "void and unenforceable," N.C.G.S. § 75-41(e), thus giving rise to a claim for unjust enrichment or restitution.

141. By reason of Defendants' wrongful conduct, Defendants have benefited from receipt and maintenance of improper funds, and under principles of equity and good conscience, Defendants should not be permitted to keep this money.

142. As a result of Defendants' conduct it would be unjust and/or inequitable for Defendants to retain the benefits of its conduct without restitution to Plaintiff and the Class. Accordingly, Defendants must account to Plaintiff and the Class for their unjust enrichment.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that the Court:

(a) Issue an order certifying the Classes defined above, appointing the Plaintiff as Class representative, and designating Milberg Coleman Bryson Phillips Grossman, PLLC and Wittels McInturff Palikovic as Class Counsel;

(b) Find that Defendants have committed the violations of law alleged herein;

(c) Determine that Defendants have been unjustly enriched as a result of their wrongful conduct, and enter an appropriate order awarding restitution and monetary damages to the Nationwide Class or, alternatively, the State Classes;

(d) Enter an order granting all appropriate relief including injunctive relief on behalf of the State Classes under the applicable state laws;

(e) Render an award of compensatory damages of at least $100,000,000, the exact amount of which is to be determined at trial;

(f) Render an award of nominal damages;

(g) Issue an injunction or other appropriate equitable relief requiring Defendants to refrain from engaging in the deceptive practices alleged herein;

(h) Issue an injunction declaring that Nord Security's automatic renewal clause is "void and unenforceable" as required by N.C.G.S. § 75-41(e);

(i) Declare that Nord Security's automatic renewal clause is "void and unenforceable" as required by N.C.G.S. § 75-41(e);

(j) Declare that Defendants have committed the violations of law alleged herein;

(k) Render an award of punitive damages;

(l) Enter judgment including interest, costs, reasonable attorneys' fees, costs, and expenses; and

(m) Grant all such other relief as the Court deems appropriate.

Dated: July 31, 2024
New York, New York

WITTELS MCINTURFF PALIKOVIC

_/s/ J. Burkett McInturff_____
J. Burkett McInturff*
Jessica L. Hunter*
Ethan D. Roman*
305 BROADWAY, 7TH FLOOR
NEW YORK, NEW YORK 10007
Tel: (914) 775-8862
Fax: (914) 775-8862
jbm@wittelslaw.com
jlh@wittelslaw.com
edr@wittelslaw.com

* *Admitted Pro Hac Vice*

(Signatures continued next page)

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC

Scott C. Harris
Kathryn Anne B. Robinson
J. Hunter Bryson
900 W. MORGAN STREET
RALEIGH, NORTH CAROLINA 27603
Tel: 919-600-5000
Fax: 919-600-5035
sharris@milberg.com
krobinson@milberg.com
hbryson@milberg.com

Co-Counsel for Plaintiff and the Proposed Class